Θεωρία Αριθμών (2018-2019)

Φροντιστηριακές ασκήσεις #1, Μιγαδικοί αριθμοί

1. Στο μιγαδικό επίπεδο να σημειώσετε τις εικόνες και τις διανυσματικές ακτίνες των μιγαδικών αριθμών: $1+i, \quad 1, \quad i, \quad -2i, \quad 3+4i, \quad 3-4i, \quad 5, \quad 0.$

2. Ποιος είναι ο $\bar{z}$ όταν

$$z=-5+7i, \qquad z=-4+9i, \qquad z=4i \qquad z=11, \qquad z=-i.$$

3. Να βρείτε τα μέτρα των μιγαδικών αριθμών

$$1+i, \qquad -5i, \qquad 0, \qquad -4, \qquad (1-i)^2(1+i)^4, \qquad (3+i)/(4-3i).$$

4. Σε καθεμιά από τις παρακάτω περιπτώσεις να εκτελέσετε τις πράξεις που σημειώνονται και να γράψετε το αποτέλεσμα στη μορφή $\alpha+\beta i$ με $\alpha,\beta \in \mathbb{R}$

   - $(-4+6i)+(7-2i)$, $\qquad (4+4i)+(-8-7i)+(5+3i)$
   - $(3-2i)-(6+4i)$, $\qquad (3+2i)(4+5i)$
   - $3i(6+i)$, $\qquad (4+3i)(4-3i)$
   - $1/(1+i)$, $\qquad i^6$
   - i^2+2i+1, $\qquad (1+i\sqrt{3})^2$
   - $(3+i)/(2-i)$, $\qquad (6-i\sqrt{2})/(1+i\sqrt{2})$

5. Για έναν μιγαδικό αριθμό z να αποδείξετε ότι:

   - Ο z είναι πραγματικός, αν και μόνο αν $z=\bar{z}$.
   - Ο z είναι φανταστικός, αν και μόνο αν $z=-\bar{z}$.

6. Αν $z_1=(5-9i)/(7+4i)$ και $z_2=(5+9i)/(7-4i)$ να δείξετε ότι ο z_1+z_2 είναι πραγματικός αριθμός, ενώ ο z_1-z_2 είναι φανταστικός αριθμός.

7. Να βρείτε τους $x,y \in \mathbb{R}$ για τους οποίους ισχύει

   - $(x+y)+(x-y)i=3-i$
   - $(3-2i)^2-(x+yi)=x-yi$
   - $((1+i)/(1-i))^2+1/(x+yi)=1+i$

8. Να λύσετε, για z μιγαδικό αριθμό, τις εξισώσεις

   - $\bar{z}=z^2$
   - $\bar{z}=z^3$

Θεωρία Αριθμών (2018-2019)

Φροντιστηριακές ασκήσεις #2, Μιγαδικοί αριθμοί (Συνέχεια)

1. Να λύσετε, για z μιγαδικό αριθμό, τις εξισώσεις:
$$z^2 - 3z + 2 = 0, \qquad z^2 - 2z + 3 = 0, \qquad z + 1/z = 1.$$

2. Να βρείτε τους μιγαδικούς $z = x + yi$ (με $x, y \in \mathbb{R}$) για τους οποίους ισχύει:
$$|z^2| = z^2, \qquad |z - 1| = z, \qquad |z + i| = 2\bar{z}.$$

3. Να βρείτε πού ανήκουν οι μιγαδικοί z για τους οποίους
$$|z| = 1, \qquad |z - i| = 1, \qquad 1 < |z| < 2, \qquad |z| \geq 2.$$

4. Αν για τους μιγαδικούς z ισχύει $|z| = 1$, να βρείτε που ανήκουν οι εικόνες των μιγαδικών w με $w = 2z + 1$. Με άλλα λόγια, περιγράψτε το σύνολο
$$A = \{2z + 1 : z \in \mathbb{C},\ |z| = 1\}.$$

5. Να γράψετε σε τριγωνομετρική μορφή τους μιγαδικούς:
$$1 + \sqrt{3}i, \qquad 1 - \sqrt{3}i, \qquad -1 - \sqrt{3}i, \qquad -1 + \sqrt{3}i, \qquad 4, \qquad -4.$$

6. Να υπολογίσετε την παράσταση $((1 + i)/(\sqrt{2}))^6$.

7. Αν $z = (1 + i\sqrt{3})/2$ να υπολογίσετε τον z^{2017}.

8. Να ερμηνεύσετε γεωμετρικά τη διαίρεση ενός μιγαδικού z με i.

9. Αν $\theta \in \mathbb{R}$ και $z = \cos\theta + i\sin\theta$ να αποδείξετε ότι για κάθε $n \geq 1$ ισχύει
$$z^n + (1/z)^n = 2\cos(n\theta), \qquad z^n - (1/z)^n = 2i\sin(n\theta).$$

10. Αν $n \geq 2$ είναι θετικός ακέραιος και $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$ να αποδείξετε ότι
$$1 + \omega + \omega^2 + \omega^3 + \ldots + \omega^{n-1} = 0, \qquad 1 \cdot \omega \cdot \omega^2 \cdot \ldots \cdot \omega^{n-1} = (-1)^{n-1}.$$

11. Να λύσετε τις εξισώσεις και να παραστήσετε τις λύσεις στο μιγαδικό επίπεδο:
$$z^3 = 1, \qquad z^4 = 1, \qquad z^6 = 1.$$

12. Να λύσετε, για z μιγαδικό αριθμό, τις εξισώσεις:
$$z^3 = -i, \qquad z^4 = 16(\cos(4\pi/3) + i\sin(4\pi/3)), \qquad z^6 = -64,$$
$$z^3 = 1 - i, \qquad z^7 + 1 = 0, \qquad z^4 + 5z^2 + 4 = 0.$$

Θεωρία Αριθμών (2018-2019)

Φροντιστηριακές ασκήσεις #3, Μαθηματική Επαγωγή, Διαιρετότητα

1. Δείξτε ότι για κάθε θετικό ακέραιο n ισχύει $n! \leq n^n$.

2. Δείξτε ότι για κάθε θετικό ακέραιο n ισχύουν τα ακόλουθα:
$$1 + 3 + 5 + \cdots + (2n-1) = n^2, \qquad 1 + 4 + 7 + \cdots + (3n-2) = \frac{n(3n-1)}{2}.$$

3. Να δείξετε ότι υπάρχει θετικός ακέραιος N έτσι ώστε να ισχύει $2^n > n^3$ για κάθε $n \geq N$.

4. Να δείξετε ότι για κάθε θετικό ακέραιο n ισχύουν
$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}, \qquad 1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$$

5. Να εκτελεσθεί η Ευκλείδεια Διαίρεση μεταξύ των ακεραίων a και b, όταν:
$$a = 352,\ b = 7, \quad a = 352,\ b = -7, \quad a = -352,\ b = 7, \quad a = -352,\ b = -7.$$

6. Έστω $a, b \in \mathbb{Z}$, $b \neq 0$. Να δείξετε ότι υπάρχουν μοναδικοί ακέραιοι q, r έτσι ώστε:
$$a = bq + r, \qquad -\frac{|b|}{2} < r \leq \frac{|b|}{2}$$

7. Να δείξετε ότι το γινόμενο δύο διαδοχικών ακεραίων είναι άρτιος αριθμός. Επίσης να δείξετε ότι το γινόμενο τριών διαδοχικών ακεραίων είναι πολλαπλάσιο του 3. Επιπλέον να εξετασθεί αν το γινόμενο n το πλήθος διαδοχικών ακεραίων είναι πολλαπλάσιο του n για κάθε θετικό ακέραιο n.

8. Δείξτε ότι αν ο n είναι περιττός θετικός ακέραιος τότε το 11 διαιρεί τον $10^n + 1$, ενώ αν ο n είναι άρτιος θετικός ακέραιος τότε το 11 διαιρεί τον $10^n - 1$.

9. Βρείτε την 2-αδική και την 3-αδική αναπαράσταση του αριθμού 100.

10. Έστω ότι ο θετικός ακέραιος n έχει 6-αδική αναπαράσταση $(2052)_6$. Βρείτε τον αριθμό n.

11. Δείξτε ότι κάθε φυσικός αριθμός της μορφής $6k + 5$ έχει έναν πρώτο διαιρέτη της μορφής $6k + 5$. Σαν πόρισμα δείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $6k + 5$.

Θεωρία Αριθμών (2018-2019)

Φροντιστηριακές ασκήσεις #4, Μέγιστος Κοινός Διαιρέτης

1. Δίδεται ότι $3168 = 2^5 \cdot 9 \cdot 11$ και $15972 = 2^2 \cdot 3 \cdot 11^3$. Να βρεθεί ο Μέγιστος Κοινός Διαιρέτης και το Ελάχιστο Κοινό Πολλαπλάσιο των 3168 και 15972.

2. Να υπολογίσετε τον Μέγιστο Κοινό Διαιρέτη d και το Ελάχιστο Κοινό Πολλαπλάσιο e των αριθμών 1485 και 1745. Στη συνέχεια να βρεθούν ακέραιοι x και y έτσι ώστε:
$$d = 1485x + 1745y$$

3. Δείξτε ότι για κάθε ακέραιο m ισχύει
$$(2m + 1, 9m + 4) = 1$$

4. Έστω a, b θετικοί ακέραιοι και p ένας πρώτος αριθμός. Είναι οι ακόλουθες προτάσεις αληθείς ή ψευδείς; Για κάθε μια δώστε απόδειξη ή αντιπαράδειγμα:

   (α′) Αν $(a, p^2) = p$, τότε: $(a^2, p^2) = p^2$.

   (β′) Αν $(a, p^2) = p$ και $(b, p^2) = p^2$, τότε: $(ab, p^4) = p^3$.

   (γ′) Αν $(a, p^2) = p$ και $(b, p^2) = p$, τότε: $(ab, p^4) = p^2$.

   (δ′) Αν $(a, p^2) = p$, τότε: $(a + p, p^2) = p$.

5. Έστω m ένας ακέραιος. Να δείξετε ότι οι αριθμοί
$$6m - 1, \quad 6m + 1, \quad 6m + 2, \quad 6m + 3, \quad 6m + 5$$
είναι ανά δύο πρώτοι μεταξύ τους.

6. Έστω $a, b \in \mathbb{N}$, και υποθέτουμε ότι $(a, b) = 1$. Να δείξετε ότι:

   (α′) $(a + b, a - b) = 1$ ή 2.

   (β′) $(2a + b, a + 2b) = 1$ ή 3.

   Μπορείτε να προσδιορίσετε, για κάθε μία από τις παραπάνω περιπτώσεις πότε ακριβώς ο μέγιστος διαιρέτης έχει την τιμή 1, 2, ή 3;

7. Αν a, b είναι φυσικοί αριθμοί, να δείξετε ότι:
$$(a, b) = (a + b, [a, b])$$
όπου (c, d) συμβολίζει το Μέγιστο Κοινό Διαιρέτη και $[c, d]$ το Ελάχιστο Κοινό Πολλαπλάσιο. Ως εφαρμογή, βρείτε δύο φυσικούς αριθμούς έτσι ώστε το άθροισμά τους να είναι 798 και το ελάχιστο κοινό τους πολλαπλάσιο να είναι 10780.

Θεωρία Αριθμών (2018-2019)

Φροντιστηριακές ασκήσεις #5, Διαιρετότητα, Πρωτογενής Ανάλυση

1. Αποδείξτε ότι ο αριθμός 211 είναι πρώτος.

2. Δείξτε ότι αν ο a είναι περιττός ακέραιος τότε ο a^2 είναι της μορφής $8k+1$ και ο a^4 είναι της μορφής $16k+1$.

3. Έστω p, q, a θετικοί ακέραιοι με τους p, q διαφορετικούς πρώτους. Δείξτε ότι αν τα p και q διαιρούν τον a τότε και το pq διαιρεί τον a. Δείξτε με παράδειγμα ότι το συμπέρασμα δεν ισχύει αν τα p, q, a είναι θετικοί ακέραιοι με τον p πρώτο αλλά τον q σύνθετο.

4. Έστω p, a, b θετικοί ακέραιοι με τον p πρώτο. Δείξτε ότι αν $pb = a^2$ τότε το p διαιρεί τον b.

5. Έστω $n \geq 2$ και
$$b = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$$
η πρωτογενής ανάλυση του φυσικού αριθμού b. Δείξτε ότι η n-στή ρίζα του b είναι ρητός αριθμός αν και μόνο αν το n διαιρεί το a_i για κάθε $i = 1, 2, \ldots, m$. Σαν πόρισμα, έχουμε ότι ο $\sqrt{p}$ είναι άρρητος για κάθε πρώτο p. Πιο γενικά, σαν πόρισμα έχουμε ότι αν ο a είναι γινόμενο διακεκριμένων πρώτων τότε ο $\sqrt{a}$ είναι άρρητος.

6. Έστω $a, b, n, m \in \mathbb{N}$ με $n \geq m$. Υποθέτουμε ότι το a^n διαιρεί το b^m. Δείξτε ότι το a διαιρεί το b.

7. Βρείτε όλους τους φυσικούς διαιρέτες των αριθμών:
$$28, \quad 140, \quad 2013, \quad 1001, \quad 9999, \quad 10!, \quad \binom{30}{10}$$

8. Να περιγραφούν όλοι οι φυσικοί αριθμοί οι οποίοι έχουν ακριβώς 2, 3 ή 4 θετικούς διαιρέτες.

9. Να βρεθούν όλες οι θετικές ακέραιες λύσεις της εξίσωσης
$$m^n = n^m$$
δηλαδή να βρεθούν όλα τα ζεύγη θετικών ακεραίων αριθμών (n, m) τα οποία ικανοποιούν την παραπάνω εξίσωση.

10. Δείξτε ότι κάθε ακέραιος αριθμός μεγαλύτερος του 11 είναι άθροισμα δύο σύνθετων αριθμών.

Θεωρία Αριθμών (2018-2019)

Φροντιστηριακές ασκήσεις #6, Διοφαντικές εξισώσεις, Ακέραιοι mod n

1. Βρείτε όλες τις ακέραιες λύσεις ή αποδείξτε ότι δεν υπάρχουν ακέραιες λύσεις, για τις ακόλουθες διοφαντικές εξισώσεις

$$1485x + 1745y = 15, \qquad 102x + 1001y = 1, \qquad 60x + 18y = 97.$$

2. Έστω η διοφαντική εξίσωση

$$ax + by = c$$

όπου $a, b, c \in \mathbb{N}$. Να δείξετε ότι το σύνολο των θετικών λύσεων της παραπάνω διοφαντικής εξίσωσης είναι πεπερασμένο. Να εξετασθεί αν η διοφαντική εξίσωση

$$31x + 43y = 5$$

έχει θετικές λύσεις. Επιπλέον δείξτε ότι το σύνολο των θετικών λύσεων της διοφαντικής εξίσωση $x - y = 1$ είναι άπειρο.

3. Έστω $a_1, \ldots, a_n$ ακέραιοι όχι όλοι μηδέν και c ακέραιος. Πότε έχει η Διοφαντική εξίσωση

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$$

ακέραιες λύσεις;

4. Δείξτε ότι η κλάση υπολοίπων $[10]_{21}$ είναι αντιστρέψιμη ως στοιχείο του $\mathbb{Z}_{21}$, και βρείτε την αντίστροφη κλάση.

5. Δείξτε ότι η κλάση $[62]_{155}$ δεν είναι αντιστρέψιμη ως στοιχείο του $\mathbb{Z}_{155}$.

6. Δείξτε ότι αν $a, n \in \mathbb{Z}$ με $n \geq 1$ τότε το σύνολο

$$S = \{a, a+1, \ldots, a+n-1\}$$

αποτελεί ένα πλήρες σύστημα υπολοίπων mod n. Επίσης, δείξτε ότι υπάρχουν ακριβώς $\phi(n)$ στοιχεία στο S που είναι πρώτα με το n.

7. Πόσοι ακέραιοι μεταξύ του 1368 και του 2018 είναι πρώτοι με το 21;

8. Δείξτε ότι

$$2^{20} - 1 \equiv 0 \bmod 41, \qquad 2^{50} \equiv 4 \bmod 7,$$
$$41^{65} \equiv 6 \bmod 7, \qquad 1! + 2! + 3! + \ldots + 100! \equiv 9 \bmod 12,$$
$$1^5 + 2^5 + 3^5 + \ldots + 100^5 \equiv 0 \bmod 4.$$

Θεωρία Αριθμών (2018-2019)

Φροντιστηριακές ασκήσεις #7, Ακέραιοι mod n

1. Δείξτε ότι για κάθε $n \in \mathbb{N}$, ο αριθμός
$$\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$$
είναι ακέραιος.

2. Βρείτε όλους τους φυσικούς αριθμούς n για τους οποίους ο αριθμός $\phi(n)$ είναι περιττός.

3. Να δείξετε ότι υπάρχουν θετικοί ακέραιοι n έτσι ώστε $\phi(n) = 2, 4, 6, 8, 10, 12$.

4. Να δείξετε ότι δεν υπάρχει θετικός ακέραιος n έτσι ώστε $\phi(n) = 14$.

5. Να δείξετε ότι αν $m \in \mathbb{N}$, τότε το σύνολο των θετικών ακέραιων λύσεων της εξίσωσης
$$\phi(x) = m$$
είναι πεπερασμένο.

6. Έστω $n \in \mathbb{Z}$ με $n \geq 2$ και $X = \{x_1, x_2, \cdots, x_n\}$ ένα πλήρες σύστημα υπολοίπων mod n. Δείξτε ότι αν n περιττός τότε
$$\sum_{i=1}^{n} x_i \equiv 0 \pmod{n}$$
ενώ αν n άρτιος τότε
$$\sum_{i=1}^{n} x_i \equiv n/2 \pmod{n}.$$

7. Δείξτε ότι: $11 \mid 10! + 1$ και $13 \mid 12! + 1$

8. Να βρεθούν τα υπόλοιπα των διαιρέσων:
$$\frac{16!}{19} \quad \& \quad \frac{5!25!}{31} \quad \& \quad \frac{7 \cdot 8 \cdot 9 \cdot 15 \cdot 16 \cdot 17 \cdot 23 \cdot 24 \cdot 25 \cdot 43}{11} \quad \& \quad \frac{5^{100}}{7} \quad \& \quad \frac{6^{2000}}{11}$$

9. Δείξτε ότι:
$$3^{999999999} \equiv -1 \pmod{7} \qquad \& \qquad 2^{1000000} \equiv 1 \pmod{17}$$

10. Δείξτε ότι για κάθε $n \in \mathbb{N}$:
$$42 \mid n^7 - n \qquad \& \qquad 30 \mid n^9 - n$$

11. Δείξτε ότι αν $p > 2$ είναι πρώτος, τότε
$$(p-2)! \equiv 1 \pmod{p}$$

Θεωρία Αριθμών (2018-2019)

Φροντιστηριακές ασκήσεις #8, Συστήματα γραμμικών ισοτιμιών, Τάξη ακεραίου $\mathsf{mod}\ n$

1. Βρείτε όλες τις λύσεις στο $\mathbb{Z}$, ή αποδείξτε ότι δεν υπάρχουν ακέραιες λύσεις, για τις ισοτιμίες:

$$5x \equiv 2 \pmod{8}, \qquad 13x \equiv 6 \pmod{26}, \qquad 3x \equiv 9 \pmod{30}.$$

2. Δείξτε ότι για κάθε $k \geq 2$, υπάρχουν k το πλήθος διαδοχικοί ακέραιοι, κάθε ένας από τους οποίους διαιρείται από τετράγωνο αριθμού > 1.

3. Για ποιές τιμές του c, όπου $0 \leq c \leq 29$, έχει λύσεις η ισοτιμία $12\,x \equiv c \pmod{30}$ Όταν υπάρχουν λύσεις, πόσες ανισότιμες λύσεις (mod 30) υπάρχουν;

4. Βρείτε έναν αριθμό ο οποίος είναι πολλαπλάσιο του 11 και δίνει υπόλοιπο 1 όταν διαιρεθεί με τους αριθμούς $2, 3, 5$, και 7.

5. Βρείτε όλες τις λύσεις στο $\mathbb{Z}$ για το σύστημα γραμμικών ισοτιμιών

$$(\Sigma) \qquad \begin{cases} x \equiv 32 \pmod{8} \\ x \equiv -6 \pmod{15} \\ x \equiv 2 \pmod{7} \end{cases}$$

6. Βρείτε όλες τις λύσεις στο $\mathbb{Z}$ για το σύστημα γραμμικών ισοτιμιών

$$(\Sigma) \qquad \begin{cases} 2x \equiv 14 \pmod{10} \\ 5x \equiv 5 \pmod{15} \\ 3x \equiv 2 \pmod{8} \end{cases}$$

7. Βρείτε τις τάξεις mod 16 των ακεραίων $3, 5, 7$ και 9.

8. Βρείτε τις τάξεις των στοιχείων του $\mathsf{U}(\mathbb{Z}_9)$ και $\mathsf{U}(\mathbb{Z}_{10})$, όπου $\mathsf{U}(\mathbb{Z}_n)$ είναι το σύνολο των αντιστρεφίμων στοιχείων του $\mathbb{Z}_n$.

9. Έστω $n \geq 2$ ακέραιος και a, b ακέραιοι με $ab \equiv 1 \pmod{n}$. Δείξτε ότι:

$$(a, n) = 1, \qquad (b, n) = 1, \qquad \mathsf{ord}_n(a) = \mathsf{ord}_n(b).$$

10. Έστω a, m ακέραιοι με $a \geq 2, m \geq 2$. Θέτουμε $n = a^m - 1$. Δείξτε ότι

$$(a, n) = 1, \qquad \mathsf{ord}_n(a) = m$$

και ακολούθως να συμπεράνετε ότι $m \mid \phi(a^m - 1)$.

Θεωρία Αριθμών (2018-2019)

Φροντιστηριακές ασκήσεις #9, Τάξη ακεραίου $\mathsf{mod}\ n$, Πρωταρχικές ρίζες

1. Έστω a, n ακέραιοι με $n \geq 1$ και $(a, n) = 1$. Να δειχθεί ότι ο θετικός ακέραιος x είναι λύση της ισοτιμίας
$$a^x \equiv 1 \pmod{n}$$
αν και μόνο αν $\mathsf{ord}_n(a) \mid x$. Σαν εφαρμογή, να βρεθούν όλες οι θετικές λύσεις της ισοτιμίας $2^x \equiv 1 \pmod{7}$.

2. Έστω $n \geq 3$ ακέραιος. Δείξτε ότι $(n-1, n) = 1$ και ότι $\mathsf{ord}_n(n-1) = 2$. Σαν συνέπεια, να συμπεράνετε ότι $2 \mid \phi(n)$.

3. Βρείτε, αν υπάρχουν, πρωταρχικές ρίζες $(\mathsf{mod}\ n)$, όπου $n = 4, 5, 10, 13, 14, 18, 20$.

4. Βρείτε πρωταρχικές ρίζες $(\mathsf{mod}\ n)$, όπου $n = 23$ και $n = 31$.

5. Δείξτε ότι αν υπάρχει μια πρωταρχική ρίζα $(\mathsf{mod}\ n)$ τότε υπάρχουν ακριβώς $\phi(\phi(n))$ ανισότιμες πρωταρχικές ρίζες $(\mathsf{mod}\ n)$.

6. Βρείτε όλες τις πρωταρχικές ρίζες $(\mathsf{mod}\ 23)$.

7. (α′) Δείξτε ότι το 3 είναι πρωταρχική ρίζα $(\mathsf{mod}\ 17)$.

   (β′) Για δοθέντα ακέραιο a με $(a, 17) = 1$ υπολογίστε τον ελάχιστο θετικό ακέραιο k ώστε $3^k \equiv a \pmod{17}$.

   (γ′) Λύστε για x ακέραιο την ισοτιμία $x^4 \equiv 13 \pmod{17}$.

8. Έστω p περιττός πρώτος και a ένας ακέραιος με $(a, p) = 1$. Δείξτε ότι:

   (α′) Αν $p \equiv 1 (\mathsf{mod}\ 4)$, τότε ο a είναι πρωταρχική ρίζα $(\mathsf{mod}\ p)$ αν και μόνο αν ο ακέραιος $-a$ είναι επίσης πρωταρχική ρίζα $(\mathsf{mod}\ p)$.

   (β′) Αν $p \equiv 3 (\mathsf{mod}\ 4)$, τότε ο a είναι πρωταρχική ρίζα $(\mathsf{mod}\ p)$ αν και μόνο αν $\mathsf{ord}_p(-a) = \frac{p-1}{2}$.